FRANCISCO JAVIER SANZ SALGUERO*

Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea**

Fundamental Right to the Protection of Personal Data in Latin America: Challenges Faced with the Extraterritorial Reach of the General Data Protection Regulation of the European Union

RESUMEN

Los avances en al ámbito de la informática han tenido gran impacto en el tratamiento de la información personal. Consecuencia de esa situación es la aprobación y reciente aplicación (2018) del Reglamento General de Protección de Datos de la Unión Europea (RGPD), normativa a la que se le atribuye una vocación de extraterritorialidad. La importancia del Reglamento se encuentra asociada con la naturaleza de derecho fundamental reconocida en Europa a la tutela de los datos personales. En contraste, pese a la preocupación por la cuestión en América Latina y su desarrollo en el marco constitucional y legal, en esta región ese desarrollo tiene un carácter asimétrico, escenario

* Doctor en Derecho, Pontificia Universidad Católica de Valparaíso (Chile). Abogado, Universidad Externado de Colombia. Académico investigador en la Universidad Santo Tomás, Santiago de Chile. ORCID: https://orcid.org/0000-0002-3082-3863. Contacto: fjsanzsalguero@hotmail.com.

** Este trabajo es parte del proyecto Fondecyt de Iniciación n.° 11221089, "Desafíos para la modernización de la Ley n.° 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", financiado por la Agencia Nacional de Investigación y Desarrollo (Chile).

Recibido el 2 de febrero de 2024; aprobado el 15 de marzo de 2024.

Para citar el artículo: Sanz Salguero, F. J. "Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea", *Revista Derecho del Estado*, Universidad Externado de Colombia, n.º 62, mayo-agosto de 2025, 143-169.

DOI: https://doi.org/10.18601/01229893.n62.06

que obliga a determinar el estado del arte con respecto a esa disparidad. Los aspectos anteriores, vinculados a la revisión de otros elementos deducidos del Reglamento europeo, nos permitirán aportar a la discusión sobre los desafíos que debe enfrentar la tutela iusfundamental de los datos personales en Latinoamérica, de cara a la aplicación del RGPD.

PALABRAS CLAVE

Información personal, derechos fundamentales, América Latina, RGPD.

ABSTRACT

Advances in the field of computing have had a great impact on the processing of personal information. A consequence of this situation is the approval and recent application (2018) of the General Data Protection Regulation of the European Union (GDPR), a regulation to which an extraterritorial vocation is attributed. The importance of the Regulation is associated with the nature of the fundamental right recognized in Europe to the protection of personal data. In contrast, despite the concern about the issue in Latin America and its development in the constitutional and legal sphere, in this region this development has an asymmetrical character, a scenario that requires determining the state of the art with respect to this disparity. The above aspects, linked to the review of other elements deduced from the European Regulation, will allow us to contribute to the discussion on the challenges that the fundamental protection of personal data in Latin America must face, in view of the application of the GDPR.

KEYWORDS

Personal information, fundamental rights, Latin America, GDPR.

SUMARIO

3.2.1. Transferencia de datos a terceros países y "nivel adecuado de protección" de la información. 3.2.2. Comentarios sobre el elemento "gestión del riesgo". Conclusiones. Referencias

INTRODUCCIÓN

En el contexto de un mundo globalizado, la protección de la información personal se configura como una de las mayores preocupaciones en la sociedad actual, escenario caracterizado por los permanentes avances en la informática y las telecomunicaciones. En este ambiente de cambio, dicha inquietud tiene su mayor expresión en el derecho europeo con la aprobación y reciente aplicación (2018) del Reglamento General de Protección de Datos de la Unión Europea (en adelante, RGPD o "el Reglamento")[1], legislación más avanzada en esta materia. La generación del anterior instrumento va en sintonía con el carácter de derecho fundamental otorgado por el ordenamiento de esta comunidad política a la tutela de los datos personales. La puesta en marcha del RGPD adquiere mayor relevancia, teniendo en cuenta la vocación de eficacia extraterritorial que se le reconoce. Aunque América Latina no ha sido ajena a esa preocupación sobre el resguardo de la información personal (aspecto que se ve reflejado en el marco de su desarrollo constitucional y legal), este desarrollo ha tenido un carácter dispar, realidad que nos impulsa a examinar el estado de la cuestión en el contexto de esa asimetría. Es preciso asociar las consideraciones anotadas a otros factores deducidos del RGPD, factores que, en conjunto, deben ser tenidos en cuenta por los ordenamientos latinoamericanos de cara a los desafíos que propone la aplicación del Reglamento europeo.

Con las anteriores premisas, en su primera etapa la investigación examina el estado del arte de la protección de la información personal en América Latina, concluyendo con la explicación de la naturaleza iusfundamental de esta protección como característica transversal en la esfera regional. En su segunda parte, el trabajo avanza revisando el alcance extraterritorial del RGPD, labor que involucra el análisis del artículo 3 del Reglamento (norma que aborda su espectro de aplicación territorial), junto con la revisión de los desafíos que ha debido enfrentar la aplicación del citado estatuto al momento de hacer efectiva dicha vocación. La fase final del documento (teniendo como punto de partida los antecedentes en la relación entre los Estados latinoamericanos y europeos en la esfera del tratamiento de los datos personales) se concentra en dos elementos que los ordenamientos de América Latina deben tener en cuenta, de cara a los desafíos que propone la aplicación del RGPD: por un

1 La identificación completa del instrumento es "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)".

lado, tenemos la transferencia de datos a terceros países y el *nivel adecuado de protección* de la información y, por otro lado, el factor *gestión del riesgo*. Por último, en cuanto a su estructura la investigación está dividida en una introducción, tres apartados principales y las conclusiones.

1. DERECHO FUNDAMENTAL A LA PROTECCIÓN DE LOS DATOS PERSONALES EN AMÉRICA LATINA

Comprender el impacto en el ámbito regional del alcance extraterritorial del RGPD respecto al derecho fundamental a la protección de los datos personales exige inicialmente examinar el estado del arte de este derecho. Para lograr esta pretensión, a continuación reflexionamos sobre el momento en que se manifiesta la preocupación por el tratamiento de los datos personales en América Latina, y avanzamos en el estudio del estado de la cuestión en sí, explicando el carácter asimétrico de la atención normativa de la tutela a la información personal, concluyendo con la justificación de la naturaleza iusfundamental de esta protección (como característica transversal en la esfera latinoamericana).

1.1. Aspectos preliminares

Advirtiendo la relación género-especie existente entre la protección de la privacidad y el resguardo de los datos personales, vínculo en donde el segundo posee un carácter autónomo respecto del primero[2], a nivel universal y en especial a partir de los inicios de la llamada época de la información[3] el interés por el tratamiento de la información personal ha sido permanente. Esta preocupación no es ajena a la discusión jurídica en América Latina. En efecto, desde principios del siglo XXI e influenciados por la Directiva Europea 95/46/CE (estatuto predecesor del RGPD) y en una perspectiva cronológica

2 No obstante la protección de los datos personales puede entenderse como un derecho autónomo respecto de la privacidad, no es independiente respecto de su naturaleza. Esta afirmación, se desprende por ejemplo al revisar la jurisprudencia del Tribunal Constitucional español, la cual estimó parcialmente un amparo con relación a las hemerotecas de un periódico, identificando la relación del derecho al olvido como una expresión del derecho a la protección de la información personal, pero también respecto al derecho a la vida privada (Tribunal Constitucional español, "Sentencia 58/2018", 2018 FJ 5). Zárate Rojas, S. "Protección de datos y el criterio de expectativas de privacidad como concepto jurídico delimitador en la jurisprudencia chilena", en María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021, 657-658.

3 Pérez Gómez, A. "Educarse en la era digital. Adelanto del nuevo libro de Ángel Pérez Gómez (Separata)", en *Sinéctica Revista Electrónica de Educación*, ITESO, Universidad Jesuita de Guadalajara, n.° 40, enero-junio de 2013, 47-72, 48.

(del más antiguo al más reciente), México[4], Argentina[5], Uruguay[6], Perú[7] y Colombia[8] desarrollaron sus propias normativas encargadas de la protección de los datos personales. No obstante, entre aquellos Estados con leyes sobre tutela de datos, solo Argentina y Uruguay han sido considerados seguros para la transferencia de esta clase de información[9]. En el caso chileno, el interés por el resguardo de la vida privada o privacidad y, consecuentemente, la protección de los datos personales se ha manifestado a través de la continua regulación normativa, con dos hitos clave. En primer lugar, tenemos la Ley 19.628 de 1999 (o LPD) [estatuto que en su curso parlamentario surgió bajo la pretensión de tutelar la vida privada, pero que luego de un complejo trámite legislativo terminó limitándose al tratamiento de los datos personales[10]][11]. En segundo lugar, observamos la Ley 21719 que "regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales", aprobada por el Parlamento chileno[12] y publicada el 13 de diciembre del 2024, estatuto cuya vigencia está diferida hasta el 1.° de diciembre del 2026.

Con antelación al inicio del desarrollo normativo en la esfera regional, en el ámbito global ya se habían generado instrumentos internacionales que involucraban a países latinoamericanos. Estos mecanismos contienen disposiciones sobre privacidad e intimidad, e impactaron en el tratamiento de la información personal, sirviendo de sustento jurídico para alcanzar su tutela a través de los órganos jurisdiccionales competentes y de base para el trabajo legislativo. Entre las disposiciones más relevantes tenemos el artículo 12 de la Declaración Universal de los Derechos Humanos (1948), el artículo 5 de la Declaración Americana de los Derechos y Deberes del Hombre (1948), el artículo 17 del Pacto Internacional sobre Derechos Civiles y Políticos (1966), el artículo 11 de la Convención Americana sobre Derechos Humanos (1969)

4 Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 5 de julio del 2000.

5 Ley de Protección de los Datos Personales n.° 25.326, 4 de octubre del 2000.

6 Ley de Protección de Datos Personales n.° 18331, el 11 de agosto del 2008.

7 Ley de Protección de Datos Personales n.° 29733, 3 de julio del 2011.

8 Ley Estatutaria 1581, 18 de octubre del 2012.

9 Enríquez Álvarez, L. "La visión de América Latina sobre el Reglamento General de Protección de Datos", en *Comentario Internacional*, n.° 19, 2019, 99-112, 100, DOI: 10.32719/26312549.2019.19.4.

10 Sanz Salguero, F. "Grado de equivalencia entre la protección de los datos personales y el derecho de acceso a la información pública", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, n.° 48 (1), 2017, 135-163, 136, DOI: http://dx.doi.org/10.4067/S0718-68512017000100135.

11 Sanz Salguero, F. "Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado", en *Revista Ius et Praxis*, Universidad de Talca, n.° 22 (1), 2016, 323-376, 324, DOI: http://dx.doi.org/10.4067/S0718-00122016000100010.

12 Aprobación generada el 26 de agosto del 2024.

y el artículo 16 de la Convención de Derechos del Niño (1989)[13]. Realizados los anteriores comentarios, en la siguiente parte nos enfocamos en el estado del arte en la protección de los datos personales en América Latina, en su carácter iusfundamental.

1.2. Estado de la cuestión del derecho fundamental a la protección de los datos personales en América Latina

Ciertamente, el resguardo de los datos personales no solo es un asunto de privacidad individual: la protección de esta información alcanza la categoría de derecho fundamental. Desde un punto de vista histórico-jurídico, y antecedido por la labor del Consejo de Europa en defensa de los derechos fundamentales en general[14] (a través de recomendaciones, convenios y demás instrumentos de *soft-law*[15]), en el ámbito europeo ya el Tratado de la Unión Europea (TUE) o Tratado de Maastricht de 1992 (uno de los acuerdos fundacionales de esta comunidad política[16]) reconoció la protección de los datos personales como un derecho de naturaleza iusfundamental[17], reconocimiento que se mantuvo en la Carta de los Derechos Fundamentales de la Unión Europea del 2000 (artículo 8)[18]. En el caso latinoamericano puede afirmarse que la atención normativa de la tutela a la información personal tiene un carácter asimétrico, en donde la mayoría de los Estados de la región reconoce el derecho a la protección de datos personales por referencia directa de su Constitución o como consecuencia de las decisiones adoptadas por sus órganos jurisdiccionales, fundamentalmente por medio del reconocimiento de la acción[19] del *habeas*

13 Zamudio Salinas, M. "El marco normativo latinoamericano y la ley de protección de datos personales del Perú", en *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Bogotá, n.° 1, julio-diciembre de 2012, 1-21, 6.

14 Abad Alcalá, L. "La protección de los datos personales en la jurisprudencia del Tribunal Europeo. En María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021, 172.

15 Se considera el *soft-law* como el producto de carácter jurídico carente de fuerza vinculante, pero que impacta el modo en que las obligaciones legales clásicas son aplicadas o interpretadas, circunstancia que les otorga cierta relevancia jurídica. *Ibid*., 172.

16 Firmado en Maastricht (Países Bajos) el 7 de febrero de 1992, y que entró en vigor el 1º de noviembre de 1993.

17 Cippitani, R. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", en *Revista Electrónica del Instituto de Investigaciones Jurídicas y Sociales Ambrosio Lucas Gioja*, Buenos Aires, n.° 27, diciembre 2021 – mayo 2022, 40-55, 44.

18 Proclamada por primera vez por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza (Francia).

19 Recurso o proceso constitucional. Etimológicamente significa "conserva o guarda tus datos" (Habeas: latín; Data: inglés). Gozain, O. *La defensa de la intimidad y de los datos personales a través del habeas data*, Buenos Aires, Ediar, 2001, 213.

data[20]. En este contexto, es posible identificar tres tendencias en el marco de la señalada asimetría. En primer lugar, tenemos los Estados caracterizados por el reconocimiento constitucional explícito del derecho a la protección de datos personales, grupo en donde encontramos países como México[21], Panamá[22], Perú[23] y Venezuela[24]. En segundo término, tenemos un grupo de países con reconocimiento constitucional expreso del recurso de *habeas data*, incluyendo los casos de Panamá[25], Perú[26], Colombia[27], Brasil[28] y Ecuador[29]. En tercer lugar (reiterando el vínculo género-especie presente entre la protección de la privacidad y la tutela de la información personal), tenemos un conjunto de Estados con un reconocimiento constitucional explícito del derecho a la intimidad y a la privacidad, pero no de protección de datos personales, como son los ejemplos de Brasil[30], Ecuador[31], El Salvador[32] y Honduras[33].

Con base en la naturaleza asimétrica atribuible a la atención normativa de la tutela a la información personal en el plano latinoamericano, un interrogante que surge consiste en determinar si la iusfundamentalidad de un derecho depende de su incorporación o no en una Carta Política. En relación con esta pregunta, pensamos que cuando la protección de la información personal no es reconocida expresamente en una Constitución, la idea de derechos fundamentales en sentido material justifica la denominada "cláusula abierta" de estos derechos en particular, haciendo referencia a la apertura de fuentes para considerar como parte del ordenamiento constitucional tales derechos aun cuando no se encuentren estipulados expresamente en el texto de una Carta[34]. De hecho, en el contexto regional un amplio espectro de países incluye cláusulas abiertas dentro de sus cartas políticas (con las escasas de excepciones de Cuba, Chile, México y Panamá), fenómeno que se presenta en virtud de la progresiva aplicación por los tribunales nacionales (y en particular por los

20 Zamudio. "El marco normativo latinoamericano y la ley de protección de datos personales del Perú", cit., 7-8.

21 Artículo 6, letra A, Constitución Política de los Estados Unidos Mexicanos.

22 Artículo 42, primer párrafo, Constitución Política de la República de Panamá.

23 Artículo 2, número 6, Constitución Política del Perú.

24 Artículo 28, Constitución de la República Bolivariana de Venezuela.

25 Artículo 44, Constitución Política de la República de Panamá.

26 Artículo 200, inciso 3, Constitución Política del Perú.

27 Artículo 15, Constitución Política de Colombia. Cervantes Díaz, F. "Derecho a la intimidad y habeas data", en *Revista Derecho y Realidad*, UPTC, Bogotá, n.° 13, enero-junio 2009, 27-35, 28.

28 Artículo 5, LXXII, Constitución Política de la República Federativa del Brasil.

29 Artículo 94, Constitución Política de la República del Ecuador.

30 Artículo 5, X, Constitución Política de la República Federativa del Brasil.

31 Artículo 23, numeral 8, Constitución Política de la República del Ecuador.

32 Artículo 2, Constitución de la República de El Salvador.

33 Artículo 76, Constitución de la República de Honduras.

34 Sanz, "Grado de equivalencia entre la protección de los datos personales y el derecho de acceso a la información pública", cit., 139-140.

tribunales constitucionales) de los instrumentos internacionales de derechos humanos a los efectos de su protección en el orden interno[35]. Por cierto, no sobra aclarar que la noción de *cláusula abierta* no implica una habilitación ilimitada al intérprete u órgano de la jurisdicción constitucional, para revelar un catálogo de derechos fundamentales implícitos en un texto normativo: solamente derechos cuya materialidad fundamental sea demostrable pueden poseer tal calidad[36].

Como conclusión de esta primera parte de la investigación, pese a la asimetría argumentada en el ámbito de América Latina, el denominador común en la región es la presencia del derecho fundamental a la protección de la información personal. La anterior atribución surge ya sea por el reconocimiento constitucional explícito del derecho a la tutela de los datos personales, por el reconocimiento constitucional expreso del derecho a la intimidad y a la privacidad (y, por extensión, a la protección de la información personal) o por la aplicación de la figura de la "cláusula abierta" de los derechos de naturaleza iusfundamental (dada la progresiva aplicación por los tribunales de los instrumentos internacionales de derechos humanos, a los efectos de su resguardo en el orden interno). Hecho este examen, en la segunda parte de la investigación revisamos la vocación de eficacia extraterritorial del RGPD, estudio efectuado desde la norma encargada de su marco de aplicación territorial (artículo 3), asociado a los problemas que ha debido afrontar el Reglamento al momento de aplicar dicha vocación.

2. VOCACIÓN DE EFICACIA EXTRATERRITORIAL DEL RGPD

Desde una perspectiva global, el permanente interés por la protección de la información personal es un asunto que debe vincularse con los avances alcanzados en la esfera de las telecomunicaciones y el mundo digital, factores que han tenido impacto en el desarrollo de las prácticas negociales, en los cambios organizacionales del Estado y en la modificación de la conducta de los individuos dentro del espectro del Internet[37], por mencionar algunos efectos. La aprobación y relativamente reciente aplicación (2018) del RGPD es una consecuencia de esa preocupación, configurándose en la legislación

35 Brewer-Carías, A. "La aplicación de los tratados internacionales sobre derechos humanos en el orden interno de los países de América Latina", en *Revista IIDH*, Instituto Interamericano de Derechos Humanos, San José, Costa Rica, n.° 46, julio-diciembre de 2007, pp. 219-271, 219 y 220.

36 Aldunate Lizana, E. *Derechos fundamentales*, Santiago, Legal Publishing, 2008, 49.

37 Sanz, Salguero, F. "Desafíos para la modernización de la Ley n.° 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", en *Revista CES Derecho*, Medellín, n.° 14, enero-abril de 2023, 3-16, DOI: 10.21615/cesder.6806.

más avanzada en esta materia[38]. Este hito normativo adquiere mayor relevancia, teniendo en cuenta que la aplicación directa del RGPD y su alcance extraterritorial hacen que instituciones públicas y privadas de todo el mundo deban cumplir con las obligaciones en él establecidas, incluidas las latinoamericanas[39]. Con base en la anterior reflexión, en esta parte analizamos los elementos del artículo 3 del Reglamento (norma que aborda su ámbito de aplicación territorial) y examinamos los desafíos que ha debido enfrentar el GPDR al momento de concretar la vocación extraterritorial que se le atribuye.

2.1. Aspectos preliminares

La intención de redactar el RGPD se manifestó en enero del 2012, cuando la Comisión Europea propuso una reforma a la Directiva 95/46/CE, formulándose dos objetivos: reforzar la protección del derecho a la tutela de los datos personales e impulsar la economía digital en la Unión. Precisamente, la mayor deficiencia de la Directiva 95/46/CE consistía en la falta de aplicación directa, lo cual conllevaba una ausencia de homogenización en las leyes de la comunidad de Estados[40]. Los objetivos para la creación del Reglamento van en sintonía con los avances informáticos y con el hecho de que el Reglamento Europeo y la Directiva 95/46/CE (que deroga) comparten un principio: "Las personas físicas deben tener el control de sus datos personales". De esta forma, el RGPD supone un cambio sustancial de enfoque hacia una verdadera cultura de la prevención y el resguardo de la información personal en la Unión Europea[41].

Es amplio el espectro de materias incorporadas en el RGPD. De esta manera, junto con establecer los alcances extraterritoriales (artículo 3), el Reglamento aborda sus principios, los derechos del interesado, las normas aplicables al *responsable* y al *encargado* del tratamiento, disposiciones sobre transferencias de datos personales a terceros países u organizaciones internacionales, la situación de las autoridades de control independientes (reglas y competencias), normas relativas a la cooperación y coherencia, disposiciones sobre recursos, responsabilidad y sanciones, disposiciones relativas a situaciones específicas de tratamiento, y un capítulo de "Disposiciones finales"[42]. Concentrándonos en

38 Milanés, V. "Desafíos en el debate de la protección de datos para Latinoamérica", en *Revista Transparencia & Sociedad del Consejo para la Transparencia*, Santiago, n.° 5, 2017, 13-31, 20.

39 Enríquez, "La visión de América Latina sobre el Reglamento General de Protección de Datos", cit., 100.

40 *Ibid*., 101.

41 Fuensanta Martínez, D. "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones", en *Revista Profesional de la Información*, Universidad Complutense de Madrid, n.° 27 (1), 185-194, 190.

42 Este capítulo en particular aborda la derogación de la Directiva 95/46/CE, la relación con la Directiva 2002/58/CE y la entrada en vigor y aplicación del RGPD, entre otros asuntos.

la vocación extraterritorial presente en el RGPD, y pese a que estamos haciendo referencia a un texto legal que se aplica directamente a los países miembros de la Unión Europea, a continuación profundizamos en los alcances del artículo 3 como norma que concede dicha vocación.

2.2. El RGPD y su ámbito de aplicación territorial: elementos del artículo 3 del Reglamento

El artículo 3 del RGPD es el encargado de establecer su esfera de aplicación territorial, reconociendo una inclinación de eficacia que va más allá de las fronteras de los miembros comunitarios. Esta norma incorpora al derecho positivo la doctrina expansiva del Tribunal de Justicia de la Unión Europea TJUE (originada en casuística vinculada a empresas que se dedican a ofrecer servicios exclusivamente a través de Internet[43]) y en consecuencia se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea, independientemente de que el tratamiento tenga lugar en la comunidad política o no[44].

Interpretar los alcances del artículo 3 del Reglamento exige conocer una serie de términos incorporados en dicha norma, los cuales se encuentran definidos en el artículo 4. En este sentido, tenemos la expresión *tratamiento*, que involucra cualquier operación o conjunto de operaciones realizadas sobre datos personales (de forma singular o en conjunto), ya sea por procedimientos automatizados o no, en una amplia gama de actuaciones[45]. En segundo lugar, observamos al *responsable del tratamiento* o *responsable*[46], que es el encargado de determinar los fines o medios del *tratamiento*. En tercer lugar, tenemos al *encargado del tratamiento* o *encargado*[47], quien trata la información personal "por cuenta del responsable del tratamiento". Finalmente, observamos la expresión *interesado*[48], que aborda al titular (persona física identificada o identificable) de los datos.

43 Concretamente, tenemos las sentencias C-131/12 del 13 de mayo de 2014 (asunto Google Spain), y C-230/14 del 1.° de octubre de 2015 (asunto Weltimmo).

44 Bauzá, F. "El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura", en *Ars Boni et Aequi*, n.° 15 (1), 2019, 121-148, 126.

45 Particularmente y conforme el artículo 4 numeral 2, la operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales puede involucrar "recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

46 El cual (según el artículo 4 numeral 7) puede ser una persona física o jurídica, autoridad pública, servicio u otro organismo, el cual puede actuar solo o junto con otros.

47 El cual (según el artículo 4 numeral 8) puede ser una persona física o jurídica, autoridad pública, servicio u otro organismo.

48 Artículo 4, numeral 1 del RGPD.

Teniendo claridad en las anteriores definiciones, los elementos del artículo 3 que deben observarse al momento de establecer los alcances de su vocación extracomunitaria son los siguientes:

(a) No importa si la operación o conjunto de operaciones realizadas sobre datos personales tiene lugar dentro o fuera de la comunidad política: el RGPD se aplica a ese tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión Europea.

(b) El RGPD se aplica al tratamiento de la información personal del titular (es decir, el *interesado*) que resida en la Unión Europea, por parte de un responsable o encargado no establecido en la comunidad política, siempre y cuando las actividades de tratamiento estén relacionadas con: (1) "la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago", o (2) "el control de su comportamiento, en la medida en que este tenga lugar en la Unión"[49].

(c) El Reglamento se considera aplicable al tratamiento de datos privados por parte de un responsable que no esté establecido en la comunidad de Estados, "sino en un lugar en que el Derecho de los Estados miembros sea de aplicación"[50], aspecto que demuestra que el RGPD no es ajeno a las normas de Derecho internacional público[51].

2.3. El RGPD y los desafíos de la vocación extraterritorial

La labor del TJUE ha demostrado la dificultad de emplear normas de un ordenamiento jurídico a los flujos de datos[52]. Un ejemplo en este sentido se encuentra al contrastar dos sentencias del citado tribunal, jurisprudencias que involucraban al motor de búsqueda Google y versaban sobre los alcances del "derecho al olvido". En lo central, mientras la sentencia C-131/12 del 2014 (asunto Google Spain v. AEPD, Costeja Gonzáles)[53] reconoció el "derecho al olvido" con respecto a un motor de búsqueda informática con cobertura global como Google, con posterioridad el mismo TJUE en la decisión C-507/17 del 2019 (asunto Google LLC v. CNIL)[54] restringió el espectro territorial de aplicación de la normativa, especificando que la protección de los derechos del interesado tienen cobertura dentro de la Unión Europea. Ampliando lo

49 Artículo 3, numeral 2 del RGPD.

50 Artículo 3, numeral 3 del RGPD.

51 Bauzá, "El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura", cit., 126.

52 Cippitani. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", cit., 45.

53 Tribunal de Justicia, sentencia de 13 de mayo de 2014, *Google Spain* et al. v *AEPD*, Costeja Gonzáles, C-131/12.

54 Tribunal de Justicia, sentencia de 24 de septiembre 2019, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17.

explicado en la última en la última sentencia, el Tribunal indicó que el derecho de *desreferenciación*[55] se detiene en las fronteras de la Unión Europea teniendo en cuenta dos argumentos: (1) el propósito del RGPD es hacer cumplir los derechos de las personas dentro de la comunidad de Estados y (2) el RGPD no proporciona instrumentos y mecanismos de cooperación entre las autoridades de protección de datos, como en lo que respecta al alcance del derecho de *desreferenciación* fuera de la UE[56]. De todas formas, en un sentido global la discusión jurídica sobre la posibilidad del "derecho al olvido" es un asunto extendido a todos los países conectados a internet, realidad en la que se debate sobre las condiciones y los requisitos exigibles para la admisión de acciones judiciales que pretendan la supresión de contenidos que circulan por el ciberespacio[57].

En el marco de la vocación extracomunitaria atribuida al RGPD, los desafíos que enfrenta el Derecho continental europeo en el intento de aplicar sus normas más allá de las fronteras ha generado reacciones. En este contexto, la institucionalidad comunitaria trabaja desde el 2020 en una serie de instrumentos que apuntan a delimitar los alcances de dicha vocación. A este respecto, tenemos las "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0" (en adelante, "Recomendaciones")[58]. Este grupo de propuestas, pese a no tener un carácter vinculante, tiene la virtud de abordar un punto que afecta a Estados extracomunitarios (hipótesis que, por cierto, incumbe a los países de América Latina): las Recomendaciones reconocen en el capítulo V del RGPD, encargado de regular las transferencias de datos personales a *terceros países*[59], la condición de que

55 Con el principio de la *desreferenciación* de Google, se trata de eliminar del buscador un resultado que perjudica la imagen y reputación del afectado. Se trata, por tanto, de un proceso de "limpieza" de resultados negativos sobre una persona o empresa, una marca, un producto, etc. Disponible en https://www.net-wash.fr/es/desreferenciacion-de-google/ [consultado el 15 de mayo de 2023].

56 Uzan-Naulin, J. "The (Extra) Territorial Scope of the GDPR: The Right to Be Forgotten", en *FASKEN, Privacy and Cybersecurity Bulletin*, noviembre 28, 2019. Disponible en https://www.fasken.com/en/knowledge/2019/11/the-extra-territorial-scope-of-the-gdpr/ [consultado el 20 de agosto de 2023].

57 Anguita Ramírez, P. "El derecho al olvido en la jurisprudencia de la Corte Suprema", en María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021, 499.

58 "Recomendaciones" que tienen su origen en la sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems II (C-311/18).

59 La noción de "tercer país" abarca cualquiera que no sea un Estado miembro del Espacio Económico Europeo, que incluye a los Estados miembros de la Unión Europea y a Islandia, Noruega y Liechtenstein. Disponible en Anexo 1: Definiciones, Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0, disponible en https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_es.pdf [consultado el 20 de junio de 2023].

la transferencia no debe menoscabar el nivel de protección de las personas físicas garantizado por el mismo Reglamento[60]. En este sentido, creemos que los progresos que se logren en la implementación efectiva de las Recomendaciones permitirá avanzar en la definición de los estándares que deben cumplir las normas internas de los países de la región en materia de resguardo de los datos privados, con el fin de hacerlas coherentes con las exigencias del RGPD.

3. DESAFÍOS DE LA PROTECCIÓN DE LOS DATOS PERSONALES EN AMÉRICA LATINA, DE CARA AL RGPD

No obstante la amplia regulación legal en el tratamiento de la información personal observable tanto en el contexto de la Unión Europea (a nivel de bloque) como en el ámbito de América Latina (a nivel de Estados), factor asociado al reconocimiento de su carácter iusfundamental, a la fecha no hay reglas compartidas para el intercambio transcontinental de datos[61]. Sin embargo, en el espectro del señalado intercambio, los progresos generados en la esfera de las telecomunicaciones y la informática y la consecuente circulación de flujos de información a través del ciberespacio (flujo que se vio exacerbado a partir del año 2020 debido a la propagación mundial del virus covid-19[62]) invitan a participar en el debate sobre el establecimiento de un escenario jurídico adecuado en materia de tutela de los datos personales.

Bajo esta premisa, y teniendo como punto de partida los antecedentes identificados en la relación entre los Estados latinoamericanos y los europeos, a continuación abordamos dos elementos que los ordenamientos de América Latina deben tener en cuenta, de cara a los desafíos que propone la aplicación del RGPD: hacemos referencia a la transferencia de datos a terceros países y el *nivel adecuado de protección* de la información, y al factor *gestión del riesgo*.

3.1. Protección de la información personal en América Latina y RGPD: antecedentes

En cuanto a sus antecedentes, el examen del tratamiento de los datos personales en Latinoamérica de cara al RGPD abarca dos líneas. Por un lado, tenemos el reconocimiento de instrumentos que apuntan al resguardo de la privacidad y la información personal, y que involucran tanto a Estados de la Unión

60 Sanz. "Desafíos para la modernización de la Ley n.° 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", cit., 12-13.

61 Cippitani. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", cit., 45.

62 Badillo Hermoso-Pérez, G. "Covid-19 y protección de datos personales", en Hugo Alejandro Concha Cantú y Pozas Loyo (coords.), *Análisis jurídico y seguimiento de normas emitidas durante la pandemia covid-19*, México, D. F., UNAM, 2021, 127-128.

Europea como a países extracomunitarios. En segundo lugar, observamos la descripción de mecanismos que justifican y abogan por la construcción de una disciplina común en materia de protección de datos.

Con respecto a la primera línea de estudio, Bu-Pasha[63] identifica la Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) de 1981 o Convenio 108[64], y su Protocolo adicional (adoptado en 2001). El Convenio 108 se considera el primer y único instrumento internacional jurídicamente vinculante a Estados que hacen parte de la Unión Europea, y accesible tanto para países no europeos como para Estados no miembros del Consejo de Europa, agregando que su Protocolo adicional introdujo disposiciones sobre los flujos transfronterizos de datos hacia y desde Estados no miembros, fomentando la recopilación, el procesamiento y uso legítimo de datos personales. No obstante lo relevante del instrumento, el mismo autor reconoce que todas las partes contratantes de la Convención (excepto Uruguay) conforman el Consejo de Europa, lo cual la aleja de una práctica *internacional*. En este orden de ideas, y pese a que después de la obra de Bu-Pasha un grupo reducido de países no miembros del citado Consejo adhirieron al instrumento (incluyendo dos Estados latinoamericanos que lo hicieron recién en el año 2019: México y Argentina), creemos que el limitado alcance internacional atribuido por la doctrina al Convenio 108 se mantiene[65].

En relación con la segunda línea de examen, podemos encontrar declaraciones que confirman las visiones comunes presentes en la esfera jurídica entre Estados europeos y países americanos (asociado al reconocimiento de una conexión histórica), como ocurre con la "Declaración política" suscrita en el marco de la Cumbre UE-CELAC llevada a cabo en Bruselas entre el 10 y 11 de junio del 2015 (o EU-CELAC Summit 2015), declaración que, con la premisa de alcanzar "Una asociación para la próxima generación", en su primer numeral plantea la decisión de "ahondar en nuestra duradera asociación estratégica birregional, basada en vínculos históricos, culturales y humanos, el Derecho internacional, el pleno respeto de los derechos humanos, valores comunes e intereses mutuos"[66]. Una aspecto adicional relevante de esta declaración es que desde la perspectiva americana involucra a un extenso grupo de Estados,

63 Bu-Pasha, S. "Cross-border issues under EU data protection law with regards to personal data protection", en *Information & Communications Technology Law*, n.° 26 (3), 2017, 213–228, 213 y 214, DOI: https://doi.org/10.1080/13600834.2017.1330740.

64 Firmado el 28 de enero de 1981 en Strasbourg (Francia).

65 En efecto, hasta la fecha, los únicos países no miembros del Consejo de Europa que han adherido al Convenio 108 son: Argentina, Cabo Verde, Mauricio, México, Marruecos, la Federación Rusa, Senegal, Túnez y Uruguay. Disponible en https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108 [consultado el 15 de agosto de 2023].

66 Declaración política, cumbre UE-CELAC, 10 y 11 de junio de 2015 (EU-CELAC Summit 2015), Disponible en https://www.consilium.europa.eu/media/23747/eu-celac-political-declaration_es.pdf, [consultado el 15 de agosto de 2023].

teniendo en cuenta que la CELAC (como mecanismo intergubernamental que tiene la tarea de superar desafíos en materia de fragmentación y heterogeneidad en el ámbito regional[67]) incluye 33 países latinoamericanos y caribeños.

Continuando con la segunda línea de estudio, concentrándonos en los instrumentos que abordan directamente el tratamiento de la información personal, observamos que el Acuerdo Marco Interregional de Cooperación entre la Comunidad Europea y el Mercosur firmado en 1995[68], en su artículo 18, con miras a la promoción de los intercambios de datos[69] establecía que "la cooperación deberá adoptar todas las formas que se consideren convenientes y, particularmente, [...] sistemas de intercambio de información en todas las formas adecuadas, inclusive a través del establecimiento de redes informáticas"[70], estipulando además el "respeto por la protección de los datos personales en todos aquellos ámbitos en los que se prevea intercambios de información a través de redes informáticas"[71]. Aunque en el espectro latinoamericano este pacto está circunscrito a los países que conforman el Mercosur (es decir: Argentina, Brasil, Paraguay y Uruguay[72]), su interés radica en que constituye el precedente del Acuerdo de Libre Comercio Mercosur-Unión Europea, tratado del cual existe un acuerdo de principio (anunciado el 28 de junio de 2019), pero cuyos textos definitivos no han sido finalizados, firmados ni ratificados, por lo que no han entrado en vigor.

3.2. América Latina de cara al RGPD: otros elementos que tener en cuenta en materia de protección de los datos personales

Establecida la ausencia de reglas compartidas para el intercambio transregional de datos (factor vinculado a la preocupación por sintonizar el marco jurídico en materia de protección de la información personal), y teniendo como punto de partida el contenido y las consecuencias en la aplicación del artículo 3 del RGPD (asociado a los retos reconocidos al momento de operativizar su vocación extracomunitaria), aportar a la discusión para alcanzar una relación armónica entre la disciplina europea y latinoamericana exige

67 Díaz Galán, E y Bertot Triana, H. "La Comunidad de Estados Latinoamericanos y Caribeños (CELAC): un enfoque desde la perspectiva de la integración", en *Cuadernos de Política Exterior Argentina*, Rosario, n.° 126, julio-diciembre de 2017, 47-66, 63.

68 O "Acuerdo Marco Interregional de Cooperación entre la Comunidad Europea y sus Estados Miembros, por una Parte, y el Mercado Común del Sur y sus Estados Partes, por Otra". Disponible en http://www.sice.oas.org/tpd/mer_eu/negotiations/interregional_agreement_s.asp, [consultado el 20 de julio de 2023].

69 Cippitani. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", cit., 43.

70 Artículo 18, numeral 3, letra a.

71 Artículo 18, numeral 4.

72 El Mercosur ha incorporado a Venezuela y Bolivia, encontrándose el primero actualmente suspendido del bloque y el segundo en proceso de adhesión.

revisar además otros mecanismos planteados por el ordenamiento. En este sentido, a continuación abordamos la transferencia de datos a terceros países y el *nivel adecuado de protección* de la información, finalizando esta parte examinando el factor *gestión del riesgo*.

3.2.1. Transferencia de datos a terceros países y "nivel adecuado de protección" de la información

El RGPD admite la transferencia de datos a *terceros países*, siempre y cuando la Comisión Europea considere que el sistema legal de esos Estados es capaz de ofrecer un "nivel adecuado de protección" de la información[73]. Al respecto, el Reglamento europeo tiene la virtud no sólo de facilitar las transferencias transnacionales de datos con mecanismos mejorados: además, define procedimientos, condiciones y restricciones para las transferencias de datos personales fuera del contexto comunitario, a terceros países o a un territorio o sector específico dentro de un tercer país, o a una organización internacional, previa decisión de adecuación de la citada comisión [74].

Una cuestión que surge en este punto es la de establecer qué es el *nivel de protección adecuado*: de hecho, la doctrina habla de la aparente insuficiencia para precisar esta expresión[75]. No obstante, el RGPD aporta un conjunto de criterios que apuntan a su definición[76]. En este sentido, para determinar la adecuación la Comisión Europea tiene en cuenta factores como el sistema legal existente, el derecho penal y el acceso a la justicia en el país en cuestión, las actividades de procesamiento individuales y los requisitos internacionales de derechos humanos[77]. Adicionalmente, dicho órgano ejecutivo está obligado a realizar revisiones periódicas, y tiene la aptitud de reconocer insuficiencias en el nivel de protección de datos, con la consecuente facultad de prohibir futuras transferencias de información personal en consulta con los "organismos apropiados relacionados" (organismos que incluyen al Parlamento y Consejo Europeo, así como otras entidades y "fuentes pertinentes", indica el RGPD)[78]. Respecto de los factores esgrimidos para el establecimiento del nivel de protección adecuado, el Reglamento en su considerando 104 enfatiza la

73 RGPD, considerando 103.

74 Lo anterior, conforme a los considerandos 103 a 107 y 169, y al artículo 45 del RGPD. Bu-Pasha. "Cross-border issues under EU data protection law with regards to personal data protection", cit., 222.

75 Van Den Bulck, P. "Transfers of personal data to third countries", en *ERA Forum*, n.° 18, 2017, 229–247, 230.

76 RGPD, considerandos 106 y 107.

77 Bu-Pasha. "Cross-border issues under EU data protection law with regards to personal data protection", cit., 222.

78 Myers. A. "Top 10 Operational Impacts of the RGPD: Part 4–Cross-border Data Transfers", 19 January 2016, Disponible en https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [consultado el 20 de septiembre de 2023].

importancia de la protección de los derechos humanos, en consonancia "con los valores fundamentales en los que se basa la Unión". Con base en esta directiva, la posibilidad que un tercer país[79] (hipótesis que por cierto puede incluir a un Estado latinoamericano) cumpla con los estándares exigidos para lograr ese nivel de protección adecuado depende de que posea un enfoque en el ámbito del respeto a los derechos humanos equivalente al de los Estados de la Unión Europea, cuya tradición exige el cumplimiento del artículo 6 del Tratado de la Unión Europea (TUE) junto con los instrumentos reconocidos en dicha norma (es decir, la Carta de los Derechos Fundamentales del 2000 y el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950). Simultáneamente, el criterio del respeto de los derechos humanos tiene que considerar el contexto transnacional en que se desarrolla el sistema de protección[80]. Con respecto a este contexto, aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación de unos u otros en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones, exigiéndose además un requisito clave: la adhesión del país al Convenio 108 y a su Protocolo adicional[81].

En otra disposición del RGPD dirigida a facilitar la transferencia de datos personales (artículo 46, numeral 1), se admite la transferencia de este tipo de información por parte del responsable o el encargado del tratamiento a un tercer país u organización internacional, siempre que estos últimos ofrezcan "garantías adecuadas" y "a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas". Las garantías que puede aportar este responsable o encargado para lograr la transferencia de datos no requieren "ninguna autorización expresa de una autoridad de control". Adicionalmente, el procedimiento, posible contenido y las autoridades que otorgan dichas garantías se explican en los considerandos 108 a 110, 114 y el artículo 46 (numerales 2 a 5) del Reglamento.

En este sentido, y en circunstancias particulares, se pueden asegurar las garantías adecuadas y los datos pueden transferirse a países no pertenecientes a la Unión Europea, incluso sin un requisito de adecuación[82]. Sobre esta opción, un primer ejemplo lo representa el uso de las cláusulas contractuales estándar (artículo 46), que son cláusulas modelo utilizadas para proteger los datos, y cuyo propósito es que las partes involucradas contractualmente

79 O a un territorio o sector específico dentro de un tercer país, o a una organización internacional.

80 Cippitani. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", cit., 48.

81 RGPD, considerando 105.

82 Bu-Pasha. "Cross-border issues under EU data protection law with regards to personal data protection", cit., 223.

(o "exportador" [quien pretende transferir los datos] e "importador" [quien recibe los datos]) cumplan con el RGPD[83]. Como segundo ejemplo, tenemos la aplicación de un "código de conducta" aprobado (artículo 40). Sobre esta posibilidad, teniendo en cuenta que el Reglamento Europeo no lo define, es útil acudir al concepto de la Directiva 2005/29/CE[84], estatuto conforme al cual el código de conducta es un "acuerdo o conjunto de normas no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro, en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código en relación con una o más prácticas comerciales o sectores económicos concretos". Igualmente, estos códigos tienen un carácter voluntario (solo obligan en la medida en que alguien se someta a ellos), y están en capacidad de elaborarlos las asociaciones y otros organismos representativos de categorías de responsables, empresas y grupos de empresas, así como responsables y encargados de algunas instituciones públicas[85]. Por último, un tercer ejemplo en donde es posible la transferencia a países no pertenecientes a la Unión Europea (incluso sin un requisito de adecuación) consiste en acudir a las normas corporativas vinculantes NCV (artículo 47) o Binding Corporative Rules (BCR, por sus siglas en inglés), reglas que, conforme al RGPD, constituyen políticas de resguardo de la información personal que se aplican a las transferencias de datos entre grandes corporaciones multinacionales, o grupos de empresas, y que poseen un carácter jurídicamente vinculante. Es pertinente aclarar que estas reglas no sustituyen las normas generales sobre protección de datos, por lo que las empresas del grupo deben cumplir con sus obligaciones legales y con las BCR[86]. Ligado a lo anterior, el artículo 42 establece un acuerdo para las transferencias respaldadas por "mecanismos de certificación", a condición de que los responsables o encargados del tratamiento de datos se comprometan de manera vinculante y exigible en la aplicación de las garantías apropiadas[87].

83 Las disposiciones referentes a este tipo de cláusulas se encuentran reguladas, en detalle, en la Decisión de Ejecución (UE) 2021/914 de la Comisión Europea de 4 de junio de 2021, "relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo".

84 La identificación completa del instrumento es "Directiva 2005/29/CE del Parlamento Europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) no 2006/2004 del Parlamento Europeo y del Consejo ("Directiva sobre las prácticas comerciales desleales")".

85 Roig, A. *Códigos de conducta, certificaciones y transferencias internacionales*, Barcelona, Universitat Oberta de Catalunya, 2017, 5.

86 Meroño, A. *Normas corporativas vinculantes: evolución y efectividad* (tesis de máster), Madrid, Universidad Internacional de la Rioja, Master en Protección de Datos, 2018, 9-10.

87 Myers. A. "Top 10 Operational Impacts of the GDPR: Part 4–Cross-border Data Transfers".

En este orden de ideas, un interrogante que se plantea consiste en establecer la suerte de las decisiones emanadas de órganos jurisdiccionales o autoridades administrativas que pertenezcan a un tercer país, y que ordenen a un responsable o encargado del tratamiento la transferencia o comunicación de datos. Sobre este punto, el RGPD en su artículo 48 y considerando 115 admite el reconocimiento y ejecutividad de estas decisiones siempre y cuando estén basadas en un "acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro", sin perjuicio de otros motivos para la transferencia al amparo del mismo Reglamento. Dado que no existe una disposición análoga del artículo 48 Directiva 95/46/CE (derogada, recordemos, por el RGPD), la doctrina se ha preguntado cómo en el marco del ordenamiento europeo se interpretarán y aplicarán esta disposición y sus requisitos, lo cual constituye un desafío pendiente por resolver[88].

Finalmente, reiterando las mismas excepciones establecidas en la Directiva 95/46/CE[89], el artículo 49 del Reglamento europeo admite la posibilidad de "transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional"[90] siempre y cuando se cumplan algunas situaciones o "condiciones específicas"[91]. En este sentido[92], se permiten excepciones a las decisiones de adecuación y garantía adecuadas, por ejemplo con el consentimiento explícito del interesado o para la ejecución del contrato, entre otros casos[93].

3.2.2. Comentarios sobre el elemento "gestión del riesgo"

La discusión en la búsqueda por alcanzar una armonía jurídica, a propósito de la relación entre el bloque europeo y los países latinoamericanos en materia de protección de los datos personales, exige observar el elemento *gestión del riesgo* y su impacto en el ámbito económico interregional. Como reflexión inicial, debemos destacar la incidencia que tiene el RGPD en el marco de los procesos de integración y acuerdos de libre comercio. A título ejemplar, tenemos

88 Kessler, D., Nowak, J. y Khan, S. "The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States", en *The Sedona Conference Journal*, Phoenix, n.° 17 (2), 2017, 576-611, 577.

89 Artículo 26.

90 En ausencia (dice el artículo 49) "de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes".

91 Centre for Information Policy Leadership Hunton & Williams. *The EU General Data Protection Regulation: A Guide for In-house Lawyers,* Washington, Hunton & Williams, 2016, 32-33.

92 Y conforme al artículo 49 y los considerandos 111, 112 y 113 del RGPD.

93 Bu-Pasha. "Cross-border issues under EU data protection law with regards to personal data protection", cit., 223.

el caso del Acuerdo de Asociación Chile-Unión Europea (o AA Chile-UE), suscrito el 2002[94]. En efecto, no obstante en el AAChile-UE las partes concertaron "cooperar en la protección de los datos personales" (artículo 30), poner en práctica esta directriz exige establecer de forma clara el rango de acción del RGPD. Siguiendo con el mismo país, ampliando el espectro geográfico y enfocándonos en la región Asia-Pacífico (que abarca la ribera opuesta del Pacífico, desde Rusia y Japón por el norte hasta Nueva Zelandia por el sur), teniendo en cuenta la pertenencia de Chile al Foro de Cooperación Económica Asia-Pacífico (APEC) desde el año de 1994[95], otro asunto de interés subyace en los efectos probables del RGPD en su relación con el Sistema de Reglas de Privacidad Transfronteriza del APEC (o CBPR, por sus siglas en inglés), una de las herramientas que promueve el Marco de Privacidad del APEC, el cual se aprobó en el 2004 con el fin de adoptar principios de protección a la privacidad y al mismo tiempo evitar la creación de barreras para los flujos de información[96].

Formulada la anterior reflexión, corresponde acercarnos a la noción de *gestión del riesgo*, la cual desde una perspectiva general se considera un lenguaje universal utilizado en el sector de la seguridad de la información[97], pero que al momento de vincularla al RGPD permite atribuirle alcances y un sentido jurídico más preciso. En este contexto, la Agencia Española de Protección de Datos (o AEPD)[98] expresa que está noción está formada por un conjunto de acciones ordenadas y sistematizadas, cuyo propósito es controlar las posibles (probabilidad) consecuencias (impactos) que una actividad puede tener sobre un conjunto de bienes o elementos (activos) que deben de ser protegidos. Según la misma Agencia, la gestión del riesgo precisa de un análisis, o sea, una reflexión crítica y objetiva de un tratamiento, por lo que requiere la toma de decisiones que se han de plasmar en hechos concretos (controles) que minimicen el impacto sobre los activos, hasta alcanzar niveles tolerables. Precisamente, y al concentrarse en el rol del RGPD, el señalado organismo reconoce que el Reglamento europeo exige un proceso de gestión del riesgo para los derechos y libertades de los *interesados* (es decir, de los

94 Suscrito el 8 de noviembre de 2002, y promulgado en el Decreto 28 del 28 de enero del 2003.

95 Wilhelmy, M. "La trayectoria de Chile frente a la región Asia-Pacífico", en *Estudios Internacionales*, Instituto de Estudios Internacionales, Universidad de Chile, Santiago, n.° 167, 125-141, 125 y 130.

96 Galves, P. "CBPR y la búsqueda del equilibrio en la protección de datos personales", 28 de enero del 2019. Disponible en https://niubox.legal/cbpr-y-la-busqueda-del-equilibrio-en-la-proteccion-internacional-de-datos-personales/ [consultado el 23 de enero del 2023].

97 Enríquez, "La visión de América Latina sobre el Reglamento General de Protección de Datos", cit., 102.

98 Agencia Española de Protección de Datos. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Madrid, AEPD, 2021, 12-15, disponible en https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf [consultado el 20 de agosto de 2023].

titulares de la información personal), proceso que involucra la identificación, evaluación y mitigación[99], realizadas de una forma objetiva[100], del riesgo para estos derechos y libertades en particular. En este orden de ideas, y a propósito de la expresión "mitigación", la AEPD delimita sus alcances estableciendo que dicha mitigación ha de efectuarse mediante la adopción de medidas técnicas y organizativas que garanticen y permitan demostrar la protección de los derechos en comento[101], medidas que deberán determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento[102], y ser objeto de revisión y actualización cuando sea necesario. Igualmente, el RGPD incorpora de forma específica la noción de "riesgo" en un amplio espectro de sus normas[103], destacando lo expresado en el artículo 24.1 (del que se deduce la presencia del concepto "aproximación basada en el riesgo"[104]) que reza: "Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario". Finalmente, pese a que el Reglamento no establece un criterio práctico-metodológico para la gestión de los riesgos y tampoco exige requisitos explícitos de formalidad a la hora de ejecutar dicha gestión, sí formula exigencias mínimas para tratamientos que impliquen un alto riesgo, como los que se derivan de las obligaciones establecidas en los artículos 35 y 36 del RGPD.

Llevado a cabo el ejercicio de aproximación a la noción y los alcances de la *gestión del riesgo* en el marco del RGPD, en un siguiente paso es pertinente preguntarse a quién corresponde aplicar las medidas para garantizar un grado de seguridad adecuado al riesgo, a propósito del resguardo de derechos y libertades. El Reglamento responde este interrogante en su artículo 32, otorgando esta competencia al responsable y al encargado del tratamiento de la información personal. Desde la perspectiva doctrinal y en el contexto de las normas latinoamericanas sobre la protección de datos[105], un desafío

99 RGPD, considerando 77.

100 RGPD, considerando 76.

101 RGPD, artículo 24, numeral 1.

102 RGPD, considerando 76.

103 En forma específica y además del 24.1, el RGPD hace referencia al término "riesgo" en los artículos 4.24, 23.2.g, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 39.2, 49.1, por mencionar algunos.

104 Este concepto en particular se desarrolla en el "Statement on the role of a risk-based approach in data protection legal frameworks WP218" del Grupo de Trabajo del Artículo. Disponible en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf [consultado el 20 de agosto de 2023].

105 Enríquez, "La visión de América Latina sobre el Reglamento General de Protección de Datos", cit., 104.

lo representa el enfoque de la gestión de riesgos otorgado a nivel regional, enfoque tradicionalmente aplicado por la mayoría de las empresas a la protección de sus propios activos patrimoniales, y no dirigido a la protección de derechos y libertades. Un ejemplo de los retos que superar a partir de esta costumbre es el hecho de que el grueso del tejido productivo en América Latina lo representan pequeñas y medianas empresas (pymes)[106], unidades incapaces de implementar las medidas técnicas y organizacionales para cumplir con lo dispuesto en el RGPD, con una eficiente gestión de riesgos y evaluaciones de impacto. Este contexto desafiante se torna más complejo, teniendo en cuenta el rol que cumple el comercio electrónico dentro de la actividad negocial de estas unidades productivas, y el impacto generado con la creciente utilización de canales de venta digitales, factores vinculados con los riesgos inherentes a la recopilación y gestión de datos personales de los clientes. Frente a estos escenarios, compartimos la opinión de Enríquez Álvarez sobre la importancia de la cooperación de la Unión Europea para desarrollar o adaptar metodologías de evaluación de riesgos basadas en el Reglamento, ajustables a las legislaciones sobre protección de datos de los países latinoamericanos[107]. Como comentario final, un insumo útil que tener en cuenta, surgido de la propia experiencia regional, es el tratamiento de la *gestión del riesgo* en el caso colombiano. Esta experiencia se encuentra respaldada en una regulación robusta sobre las normas corporativas vinculantes (NCV), abordando (en el Decreto 255 de 2022[108]) su definición, objeto, requisitos y ámbito de aplicación de estas reglas. Esa expresión legal vincula a Colombia a una de las últimas tendencias internacionales en materia de protección de datos personales[109]. Siguiendo con la situación de estas normas en particular en el país suramericano, observamos el rol de la Superintendencia de Industria y Comercio[110], organismo descentralizado de naturaleza técnica que ha

106 Un ejemplo del impacto de este sector productivo en América Latina, lo constituye la presencia de 12,9 millones de estas empresas hacia el año 2021, distribuidas en 17 países de la región, de las cuales el 92,1% son micro, 6,3% pequeñas y otro 1,6% corresponden a medianas empresas. Ibarra, G. y Vullinghs, S. *Panorama digital de las micro, pequeñas y medianas empresas (mipymes) de América Latina 2021*, Santiago de Chile, GIA Consultores, 2021, 14.

107 Enríquez, "La visión de América Latina sobre el Reglamento General de Protección de Datos", cit., 108.

108 La identificación completa de la norma es "Decreto 255 de 2022 (febrero 23), por el cual se adiciona la sección 7 al capítulo 25 del Título 2 de la parte 2 del Libro 2 del Decreto 1074 de 2015, Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países".

109 Revista digital Progreso, *Modificaciones al régimen de protección de datos en Colombia*, n.° 28, junio 2022, en https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/modificaciones-al-regimen-de-proteccion-de-datos-en-colombia/ [consultado el 20 de enero de 2025].

110 Organismo de carácter técnico con personería jurídica, que goza de autonomía administrativa, financiera, presupuestal y cuenta con patrimonio propio, adscrito al Ministerio de Comercio, Industria y Turismo, que hace parte del sector descentralizado por servicios, de la Rama

formulado conceptos con respecto a los alcances, el carácter alternativo y la responsabilidad de las partes en el marco de aplicación de las NCV[111].

CONCLUSIONES

Desde una perspectiva global y como consecuencia de los avances alcanzados en el último tiempo en la esfera de la informática y las telecomunicaciones, la protección de la información personal se ha transformado en una de las mayores preocupaciones en la sociedad actual. La inquietud esgrimida tiene su mayor expresión con la aprobación y reciente aplicación del RGPD, estatuto que, además de configurarse como la norma más avanzada en la materia, posee una vocación de eficacia extraterritorial capaz de otorgarle alcances que superan las fronteras europeas. A partir de esa vocación, no obstante que los ordenamientos jurídicos de América Latina no han sido ajenos a la preocupación señalada, un interrogante que se plantea consiste en cómo afrontar el tratamiento y resguardo de los datos personales en la relación entre el bloque europeo y los países latinoamericanos.

En este orden de ideas, la pretensión de aportar al debate sobre los desafíos que debe enfrentar la tutela de la información personal en el ámbito regional, a propósito del alcance extraterritorial atribuido al RGPD, exigió inicialmente revisar el estado de la cuestión de la protección de los datos personales en América Latina en su carácter iusfundamental. En este escenario, pese a la naturaleza asimétrica atribuible a la atención normativa, el denominador común identificado es la presencia transversal del derecho fundamental a la protección de la información personal. Esta iusfundamentalidad puede surgir por el reconocimiento constitucional explícito del derecho a la tutela de los datos personales, por el reconocimiento constitucional expreso del derecho a la intimidad y a la privacidad o por la aplicación de la figura de la "cláusula abierta" de los derechos fundamentales.

Definido (dentro del marco regional) el carácter de derecho fundamental atribuible a la tutela de los datos personales, en una segunda fase de la investigación nos concentramos en la vocación de eficacia extraterritorial del RGPD. Como primera parte del análisis, concluimos que la eficacia del Reglamento más allá de las fronteras de los miembros comunitarios es posible en dos escenarios: (1) siempre se aplicará el RGPD si el establecimiento del

Ejecutiva del Poder Público en el orden nacional. Departamento Administrativo de la Función Pública de Colombia. *Manual de Estructura del Estado: Sector Comercio, Industria y Turismo*, Bogotá, Departamento Administrativo de la Función Pública, 2017, disponible en https://www1.funcionpublica.gov.co/documents/418537/7869206/11+Sector+Comercio+Industria+y+Turismo.pdf/893b8093-a5b7-4491-9a0c-3794acdfe5ec?version=1.2 [consultado el 20 de enero de 2025].

111 Superintendencia de Industria y Comercio, Concepto 23-68971 de abril de 2023. disponible en https://sedeelectronica.sic.gov.co/sites/default/files/publicaciones/Concepto_Procedencia.pdf [consultado el 21 de enero de 2025].

responsable o del encargado del tratamiento de los datos se encuentra dentro de la Unión Europea, con independencia de que la operación o el conjunto de operaciones realizadas sobre la información personal tengan lugar dentro o fuera de la comunidad política; (2) si el titular de los datos (es decir, el interesado) reside en la Unión Europea pero el tratamiento de esa información está a cargo de un responsable o encargado no establecido en la comunidad política, se aplicará el RGPD para actividades de tratamiento relacionadas con (1) la oferta de bienes o servicios (onerosa o no) a dichos interesados en la Unión o (2) al control de su comportamiento en la medida en que este tenga lugar en la Unión; adicionalmente, la norma en comento demuestra que el RGPD no es ajeno a las normas de Derecho internacional público, al estipular su aplicación al tratamiento de datos privados por parte de un responsable que no esté establecido en la comunidad de Estados, "sino en un lugar en que el Derecho de los Estados miembros sea de aplicación". No obstante la presencia de las directrices normativas explicadas, en la segunda parte del análisis observamos las dificultades que (en el espectro de los flujos de datos) ha enfrentado el RGPD en lo que concierne a la aplicación del ámbito territorial, problemática advertida en la labor del TJUE (como ocurre con la casuística vinculada con el "derecho al olvido"). Los retos que propone el escenario anterior han generado reacciones de la institucionalidad comunitaria, materializadas en instrumentos como las "Recomendaciones 01/2020", herramienta que (pese a no tener un carácter vinculante) constituye un esfuerzo por delimitar los alcances de la vocación de eficacia extraterritorial del Reglamento, y cuya implementación efectiva creemos permitirá avanzar en la definición de los estándares que debe cumplir las normas internas de los países latinoamericanos en materia de resguardo de los datos privados, con el fin de hacerlas coherentes con las exigencias del RGPD.

Por último, y en la tercera fase de la investigación, al concentrarnos en los desafíos que impone la protección de los datos personales en América Latina de cara al RGPD, una conclusión inicial es que, pese a los vínculos históricos y económicos presentes entre Estados europeos y países americanos en materia de tratamiento de información personal, a la fecha no hay reglas compartidas para el intercambio transcontinental de datos. Esta ausencia de normas, en asocio a los retos comentados al momento de definir los alcances de la vocación de eficacia extracomunitaria del Reglamento europeo, exige agregar otros factores a la discusión. En este orden de ideas, un primer elemento que tener en cuenta lo establece el RGPD al admitir la posibilidad de transferencia de datos a *terceros países* (es decir, cualquiera que no sea un Estado miembro del Espacio Económico Europeo), siempre y cuando su sistema legal sea capaz de ofrecer un *nivel adecuado de protección* de la información, hipótesis en que alcanzar el *nivel adecuado* dependerá de que el tercer país tenga un enfoque por el respeto a los derechos humanos similar al de la Unión Europea, cumpla con los compromisos internacionales adquiridos y se encuentre adherido al Convenio

108 y a su Protocolo adicional. La posibilidad de transferencia de información a un tercer país que cumple con el nivel adecuado de protección sintoniza con la cualidad atribuida al RGPD de facilitar las transferencias transnacionales de datos, atributo que se confirma con los mecanismos presentes en los artículos 40, 42, 46 (y los considerandos 108 a 110, y 114), 47, 48 (considerando 115) y 49 del Reglamento. Finalmente, un segundo elemento que observar en esta parte del trabajo es la *gestión del riesgo*, gestión regulada expresamente por el RGPD y que apunta a los derechos y libertades de los titulares de la información personal, proceso que involucra la identificación, evaluación y mitigación del riesgo para estos derechos y libertades en particular. Precisamente, y desde el punto de vista del ordenamiento de América Latina en materia de normas sobre protección de datos, el desafío lo representa el enfoque tradicionalmente aplicado por la mayoría de las empresas a la protección de sus propios activos patrimoniales, en detrimento de la protección de derechos y libertades, contexto en que la cooperación de la Unión Europea para desarrollar o adaptar metodologías de evaluación de riesgos basadas en el Reglamento, ajustables a las legislaciones de los países latinoamericanos, cumplirá un papel relevante en la labor de armonización de las relaciones intercontinentales.

REFERENCIAS

Abad Alcalá, L. "La protección de los datos personales en la jurisprudencia del Tribunal Europeo. En María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021.

Agencia Española de Protección de Datos. *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*, Madrid, AEPD, 2021, disponible en https://www.aepd.es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf [consultado el 20 de agosto de 2023].

Aldunate Lizana, E. *Derechos fundamentales*, Santiago, Legal Publishing, 2008.

Anguita Ramírez, P. "El derecho al olvido en la jurisprudencia de la Corte Suprema", en María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021.

Badillo Hermoso-Pérez, G. "Covid-19 y protección de datos personales", en Hugo Alejandro Concha Cantú y Pozas Loyo (coords.), *Análisis jurídico y seguimiento de normas emitidas durante la pandemia covid-19*, México, D. F., UNAM, 2021.

Bauzá, F. "El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura", en *Ars Boni et Aequi*, n.° 15 (1), 2019, 121-148.

Brewer-Carías, A. "La aplicación de los tratados internacionales sobre derechos humanos en el orden interno de los países de América Latina", en *Revista IIDH*, Instituto Interamericano de Derechos Humanos, San José, Costa Rica, n.° 46, julio-diciembre de 2007, 219-271.

Bu-Pasha, S. "Cross-border issues under EU data protection law with regards to personal data protection", en *Information & Communications Technology Law*, n.° 26 (3), 2017, 213–228, DOI: https://doi.org/10.1080/13600834.2017.1330740.

Centre for Information Policy Leadership Hunton & Williams. *The EU General Data Protection Regulation: A Guide for In-house Lawyers,* Washington, Hunton & Williams, 2016.

Cervantes Díaz, F. "Derecho a la intimidad y habeas data", en *Revista Derecho y Realidad*, UPTC, Bogotá, n.° 13, enero-junio 2009, 27-35.

Cippitani, R. "Hacia un espacio Euro-latinoamericano para la protección de datos personales", en *Revista Electrónica del Instituto de Investigaciones Jurídicas y Sociales Ambrosio Lucas Gioja*, Buenos Aires, n.° 27, diciembre 2021 - mayo 2022, 40-55.

Departamento Administrativo de la Función Pública de Colombia. *Manual de Estructura del Estado: Sector Comercio, Industria y Turismo*, Bogotá, Departamento Administrativo de la Función Pública, 2017, disponible en https://www1.funcionpublica.gov.co/documents/418537/7869206/11+Sector+Comercio+Industria+y+Turismo.pdf/893b8093-a5b7-4491-9a0c-3794acdfe5ec?version=1.2 [consultado el 20 de enero de 2025].

Enríquez Álvarez, L. "La visión de América Latina sobre el Reglamento General de Protección de Datos", en *Comentario Internacional*, n.° 19, 2019, 99-112, DOI: 10.32719/26312549.2019.19.4.

Díaz Galán, E y Bertot Triana, H. "La Comunidad de Estados Latinoamericanos y Caribeños (CELAC): un enfoque desde la perspectiva de la integración", en *Cuadernos de Política Exterior Argentina*, Rosario, n.° 126, julio-diciembre de 2017, 47-66.

Fuensanta Martínez, D. "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones", en *Revista Profesional de la Información*, Universidad Complutense de Madrid, n.° 27 (1), 185-194.

Galves, P. "CBPR y la búsqueda del equilibrio en la protección de datos personales", 28 de enero del 2019. Disponible en https://niubox.legal/cbpr-y-la-busqueda-del-equilibrio-en-la-proteccion-internacional-de-datos-personales/ [consultado el 23 de enero del 2023].

Gozain, O. *La defensa de la intimidad y de los datos personales a través del habeas data*, Buenos Aires, Ediar, 2001.

Ibarra, G. y Vullinghs, S. *Panorama digital de las micro, pequeñas y medianas empresas (mipymes) de América Latina 2021*, Santiago de Chile, GIA Consultores, 2021.

Kessler, D., Nowak, J. y Khan, S. "The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery from the United States", en *The Sedona Conference Journal*, Phoenix, n.° 17 (2), 2017, 576-611.

Meroño, A. *Normas corporativas vinculantes: evolución y efectividad* (tesis de máster), Madrid, Universidad Internacional de la Rioja, Master en Protección de Datos, 2018.

Pérez Gómez, A. "Educarse en la era digital. Adelanto del nuevo libro de Ángel Pérez Gómez (Separata)", en *Sinéctica Revista Electrónica de Educación*, ITESO, Universidad Jesuita de Guadalajara, n.° 40, enero-junio de 2013, 47-72.

Revista digital Progreso, *Modificaciones al régimen de protección de datos en Colombia*, n.° 28, junio 2022. Disponible en https://www.fundacionmicrofinanzasbbva.org/revistaprogreso/modificaciones-al-regimen-de-proteccion-de-datos-en-colombia/ [consultado el 20 de enero de 2025].

Roig, A. *Códigos de conducta, certificaciones y transferencias internacionales*, Barcelona, Universitat Oberta de Catalunya, 2017.

Sanz, Salguero, F. "Desafíos para la modernización de la Ley n.° 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", en *Revista CES Derecho*, Medellín, n.° 14, enero-abril de 2023, 3-16, 3, DOI: 10.21615/cesder.6806.

Sanz Salguero, F. "Grado de equivalencia entre la protección de los datos personales y el derecho de acceso a la información pública", en *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, n.° 48 (1), 2017, 135-163, DOI: http://dx.doi.org/10.4067/S0718-68512017000100135.

Sanz Salguero, F. "Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado", en *Revista Ius et Praxis*, Universidad de Talca, n.° 22 (1), 2016, 323-376, DOI: http://dx.doi.org/10.4067/S0718-00122016000100010.

Uzan-Naulin, J. "The (Extra) Territorial Scope of the GDPR: The Right to Be Forgotten", en *FASKEN, Privacy and Cybersecurity Bulletin*, noviembre 28, 2019. Disponible en https://www.fasken.com/en/knowledge/2019/11/the-extra-territorial-scope-of-the-gdpr/ [consultado el 20 de agosto de 2023].

Van Den Bulck, P. "Transfers of personal data to third countries", en *ERA Forum*, n.° 18, 2017, 229–247.

Wilhelmy, M. "La trayectoria de Chile frente a la región Asia-Pacífico", en *Estudios Internacionales*, Instituto de Estudios Internacionales, Universidad de Chile, Santiago, n.° 167, 125-141.

Zamudio Salinas, M. "El marco normativo latinoamericano y la ley de protección de datos personales del Perú", en *Revista Internacional de Protección de Datos Personales*, Universidad de los Andes, Bogotá, n.° 1, julio-diciembre de 2012, 1-21.

Zárate Rojas, S. "Protección de datos y el criterio de expectativas de privacidad como concepto jurídico delimitador en la jurisprudencia chilena", en María Isabel Serrano Maillo (dir.). *El derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Valencia, Tirant lo Blanc, 2021.

redalyc
UAEMEX

Disponible en:
https://www.redalyc.org/articulo.oa?id=337683228006

Cómo citar el artículo

Número completo

Más información del artículo

Página de la revista en redalyc.org

Sistema de Información Científica Redalyc
Red de revistas científicas de Acceso Abierto diamante
Infraestructura abierta no comercial propiedad de la academia

Francisco Javier Sanz Salguero

Derecho fundamental a la protección de los datos personales en América Latina: desafíos ante el alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea[**]

Fundamental Right to the Protection of Personal Data in Latin America: Challenges Faced with the Extraterritorial Reach of the General Data Protection Regulation of the European Union

Revista Derecho del Estado
núm. 62, p. 143 - 169, 2025
Universidad Externado de Colombia,
ISSN: 0122-9893
ISSN-E: 2346-2051

DOI: https://doi.org/10.18601/01229893.n62.06